Europeiska unionens råd

Bryssel den 27 maj 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	25 maj 2022
till:	Rådets generalsekretariat
Komm. dok. nr:	COM(2022) 252 final
Ärende:	MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET om den fjärde lägesrapporten om genomförandet av EU:s strategi för en säkerhetsunion

För delegationerna bifogas dokument – COM(2022) 252 final.

Bilaga: COM(2022) 252 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 25.5.2022
COM(2022) 252 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om den fjärde lägesrapporten om genomförandet av EU:s strategi för en säkerhetsunion

I. INLEDNING

Rysslands anfallskrig mot Ukraina dominerar för närvarande EU:s säkerhetspolitiska agenda. Kriget hotar inte bara Ukraina, utan syftar till att skada den globala stabiliteten och säkerheten. Inom EU ger det upphov till ett antal olika säkerhetsrisker för invånarna. Nya osäkerhetsfaktorer har uppstått kring försörjningen av energi och andra råvaror, och kritisk infrastruktur kan bli mål för cyberattacker. EU:s inre trygghet och säkerhet äventyras av potentiella attacker eller olyckor till följd av kemiska, biologiska, radiologiska eller kemiska agenser i krigszonen. Miljontals människor har flytt från kriget och deras utsatthet kan snabbt utnyttjas av organiserad brottslighet t.ex. i form av människohandel med kvinnor och barn, som är särskilt utsatta.

EU har agerat beslutsamt och har stått enat inför dessa nya och potentiella hot. Effekterna av kriget har hittills främst begränsats till Ukrainas territorium, men EU har skärpt sin *vaksamhet och samordning* med ökad övervakning av hotbilden och har även arbetat för att stärka motståndskraften och säkerställa *beredskapen*.

I Versaillesförklaringen av den 10–11 mars 2022[1] betonade Europas ledare att vi måste förbereda oss för plötsliga utmaningar, bland annat genom att ”skydda oss mot en alltmer omfattande hybridkrigföring och stärka vår cyberresiliens, skydda vår infrastruktur – särskilt vår kritiska infrastruktur – och bekämpa desinformation”.

Säkerhetsunionen är central för att garantera säkerhet i EU. De fyra strategiska prioriteringar som stakas ut i strategin för EU:s säkerhetsunion[2] har direkt relevans för denna uppgift i den rådande geopolitiska situationen: i) en framtidssäkrad säkerhetsmiljö, ii) hantering av föränderliga hot, iii) skydd av människor i EU från terrorism och organiserad brottslighet och iv) ett starkt europeiskt säkerhetsekosystem. Kriget visar att det är viktigt att EU och dess medlemsstater fullständigt utnyttjar de lagstiftningsinstrument och styrmedel som redan finns tillgängliga via strategin för EU:s säkerhetsunion, som stöder samordnat EU-stöd till medlemsstaterna i olika frågor, från organiserad brottslighet och terrorism till cybersäkerhet och hybridhot.

EU:s organ för rättsliga och inrikes frågor har också intensifierat sina insatser med anledning av kriget i Ukraina och spelar en viktig roll när det gäller hotbildsbedömning och stöd till operativa insatser[3]. En annan viktig faktor är att kontinuerligt stärka Schengenområdets operativa arbete och styrning.

Denna fjärde lägesrapport om genomförandet av EU:s strategi för en säkerhetsunion är inriktad på utvecklingen under de senaste månaderna sedan Rysslands anfallskrig mot Ukraina. Den ger en översikt över vidtagna åtgärder inom alla områden av säkerhetsunionen och innehåller en bedömning av de beredskapsbehov som uppstår till följd av potentiella säkerhetshot med anledning av kriget i Ukraina. Framsteg med andra frågor rörande säkerhetsunionen redovisas i bilagan.

---

1 https://www.consilium.europa.eu/media/54782/20220311-versailles-declaration-sv.pdf.
2 COM/2020/605.
3 Gemensamt uttalande från EU:s organ för rättsliga och inrikes frågor om Ukraina | Europeiska unionens asylbyrå (europa.eu).

II. CYBERSÄKERHET OCH KRITISK INFRASTRUKTUR

Sedan kriget bröt ut har privata aktörer och kriminella aktörer gått ut med att de bedriver cyberverksamhet till stöd för den ena sidan eller den andra. Hacktivism[4] utgör ett hot på grund av risken för spridningseffekter inom EU mot kritiska tjänster, risken för attacker från officiella nätverk eller andra oförutsedda spridningseffekter. Hittills har kriget till stor del förts med konventionella medel och spridningseffekterna har varit begränsade, men det finns en verklig risk för eskalering inom detta område.

EU har därför ökat sin samordning och beredskap. Hoten från kriget visar att det är nödvändigt att bygga upp en kultur av utbyte av information och sakkunskap mellan EU, medlemsstaterna och bland cybersäkerhetsgrupperna. Det handlar bland annat om att bygga upp en gemensam integrerad lägesuppfattning mellan EU:s institutioner, organ och byråer och medlemsstaterna, särskilt för kritisk infrastruktur som krävs för att den inre marknaden ska fungera på ett smidigt sätt.

Ansvarsåläggande för cyberattacker mot Ukraina

Cyberattackerna mot Ukraina började innan det ryska angreppet. Under krigets första dagar[5] var syftet att äventyra användarkonton för Ukrainas militära personal och störa grundläggande tjänster, bland annat gränskontroller och telekommunikationer.

Den 14 januari 2022 gjorde den höga representanten ett uttalande[6] på Europeiska unionens vägnar där han fördömde cyberattackerna mot Ukraina och på nytt bekräftade EU:s entydiga stöd för Ukraina.

Den 10 maj fördömde EU och dess medlemsländer tillsammans med sina internationella partner starkt[7] Rysslands skadliga it-verksamhet mot Ukraina den 24 februari, som riktades mot satellitnätet Ka-Sat, som ägs av Viasat, och klargjorde tydligt att Ryssland stod bakom attacken. Cyberattacken fick betydande konsekvenser och orsakade utan åtskillnad kommunikationsavbrott och störningar för flera offentliga myndigheter, företag och användare i Ukraina. Den drabbade också flera EU-medlemsländer.

---

4 Ett färskt exempel på hacktivism är användning av ”protestprogram” för att sprida sabotageprogram till ryska IP-adresser via ett populärt paket med öppen källkod. Protestprogram kan ge upphov till risker i leveranskedjan och minskat förtroende för nätgemenskapen för öppen källkod. Kommissionen har klargjort att (även välmenande) cyberattacker mot Ryssland är olagliga.

5 Microsoft Special Report: *An overview of Russia’s cyberattack activity in Ukraine*; ”The hybrid war in Ukraine”, *Microsoft On the Issues*.

6 https://www.consilium.europa.eu/sv/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

7 *Ryska cyberoperationer mot Ukraina: uttalande av EU:s utrikesrepresentant på EU:s vägnar* – Consilium (europa.eu).

Vaksamhet och samordning

Övervakningen av cybersäkerhetssituationen i medlemsstaterna och vid EU-institutionerna har stärkts sedan Rysslands anfallskrig mot Ukraina inleddes. Europeiska unionens cybersäkerhetsbyrå (Enisa), Europols europeiska it-brottscentrum, incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU) och Europeiska unionens underrättelseanalyscentrum (EU Intcen) har alla bidragit till EU:s gemensamma lägesuppfattning. De bedriver bland annat regelbunden övervakning av misstänkt cyberverksamhet, såväl allmänt som inom specifika sektorer som energi, transport och luftfart, och har tagit fram bedömningar som vägledning för förebyggande åtgärder.

Samordningen och informationsutbytet med cybersäkerhetsnätverk som Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) har också intensifierats. CyCLONe består av nationella cybersäkerhetsorgan, kommissionen och Enisa. För att återspegla denna strategi internt vid EU-institutionerna kan information delas mellan alla berörda avdelningar och byråer via insatsgruppen för cyberkriser, en samordningsmekanism som omfattar Enisa, Europols europeiska it-brottscentrum och CERT EU. Det krävs ständiga ansträngningar för att säkerställa kommunikationskanaler mellan de politiska, operativa och tekniska nivåerna. Det är också nödvändigt att stärka samarbetet med nätverket av enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).

Europol har även aktiverat beredskapsprotokollet för EU:s brottsbekämpningsinsatser, som möjliggör förstärkt övervakning av cyberhot och informationsutbyte mellan ett stort antal olika berörda aktörer med målet att skapa en heltäckande bild av cyberunderrättelseverksamheten.

Utöver cyberhoten har medlemsstaterna, Europeiska utrikestjänsten och kommissionens avdelningar även intensifierat övervakningen av kritiska infrastrukturers exponering mot andra hot än cyberrelaterade hot, dvs. fysiska hot. Kritiska infrastrukturer och de enheter som driver dessa infrastrukturer kan exponeras för fysiska risker, t.ex. sabotage av statliga aktörer eller statsstödda aktörer som ett led i eventuella repressalier mot EU.

Beredskap

Beredskap när det gäller cybersäkerhet och kritiska infrastrukturers säkerhet är nu viktigare än någonsin med tanke på EU:s ökade exponering för hoten från kriget. Ett antal åtgärder har vidtagits för att öka beredskapen, däribland åtgärder som redan var inplanerade före Rysslands angrepp mot Ukraina. Det handlar bland annat om övningar, vägledning, lagstiftningsåtgärder, bland annat resiliens inom kritiska sektorer, och samarbete med partner.

Tidigt 2022 anordnade Frankrikes EU-ordförandeskap tillsammans med Europeiska utrikestjänsten (*utrikestjänsten*) och Europeiska unionens cybersäkerhetsbyrå (Enisa) en scenariebaserad övning (*Cyber Crisis Linking Exercise on Solidarity*) i syfte att öka medvetenheten på politisk nivå och stärka samarbetet mellan de operativa och politiska nivåerna i händelse av en storskalig cyberattack.

I februari offentliggjorde Enisa och CERT-EU **riktlinjer** om hur resiliensen och beredskapen ska ökas i EU[8]. I riktlinjerna uppmanas alla organisationer inom den offentliga och privata sektorn att införa en minimiuppsättning med bästa praxis för cybersäkerhet med målet att betydligt förbättra cybersäkerhetskulturen. I mars offentliggjorde CERT-EU med stöd av Enisa teknisk vägledning som uppföljning[9] och säkerhetsriktlinjer för att förbättra konfigureringen av signalapparna[10]. Dessa riktlinjer innehåller ett antal praktiska rekommendationer till organisationerna om hur de kan förbättra sitt förhållningssätt till cybersäkerhet.

Lagstiftningsinitiativ

I den rådande situationen är det viktigt att **genomföra befintlig lagstiftning** och påskynda **antagandet av initiativ under behandling**.

Kommissionen hjälper medlemsstaterna att genomföra **NIS-direktivet**[11]. Enligt direktivet ska medlemsstaterna ha lämpliga resurser, t.ex. enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och utse behöriga myndigheter. Direktivet utgör grunden för ändamålsenligt samarbete mellan medlemsstaterna. Medlagstiftarnas politiska överenskommelse om **NIS2-direktivet**[12] är ett ytterligare genombrott i insatserna för att ge EU en robust beredskapsram

NIS2 – stärka beredskapen ytterligare

- I det nya direktivet om nätverks- och informationssystem åtgärdas bister i det tidigare NIS-direktivet för att anpassa direktivet till de nuvarande behoven och göra det framtidssäkrat. I NIS2-direktivet fastställs minimiregler för ett regelverk och mekanismer för ett ändamålsenligt samarbete mellan berörda aktörer i medlemsstaterna.
- Reglerna räckvidd breddas genom att nya sektorer som är kritiska för ekonomin och samhället läggs till (t.ex. sektorerna för läkemedel och medicintekniska produkter och livsmedelsproduktion). Direktivet kommer att vara tillämpligt på alla medelstora och stora enheter som är verksamma inom dessa sektorer eller tillhandahåller tjänster som omfattas av direktivet. Offentliga förvaltningsentiteter hos nationella regeringar (utom rättsväsendet, parlament och centralbanker) och på regional nivå omfattas också. Medlemsstaterna får dessutom besluta att direktivet ska tillämpas på sådana enheter på lokal nivå.
- NIS2 kommer att utgöra grunden för riskhanteringsåtgärder för cybersäkerhet och formellt inrätta Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som kommer att stödja en samordnad hantering av storskaliga cyberincidenter.
- Genom förslaget införs även mer exakta bestämmelser om förfarandet för rapportering av incidenter, innehållet i rapporten och tidsfrister och föreskriver rättsmedel och sanktioner för att säkerställa efterlevnad.
- Medlemsstaterna kommer att ha 21 månader på sig från direktivets ikraftträdande för att införliva bestämmelserna i sin nationella lagstiftning

[8] *Boosting your Organisation's Cyber Resilience – Joint Publication*, 14.2.2022.
[9] *CERT-EU Security Guidance 22-001 – Cybersecurity mitigation measures against critical threats*.
[10] *CERT-EU Security Guidance 22-002 – Hardening Signal*.
[11] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[12] COM(2020) 823.

Utöver NIS2-direktivet är det viktigt att förhandlingarna om förslaget till **direktiv om kritiska entiteters motståndskraft**[13] slutförs så snabbt som möjligt. Så snart direktivet antas och genomförs bör kritiska entiteters motståndskraft mot ett antal hot ökas, däribland terroristattacker, insiderhot eller sabotage. Det är också viktigt att ambitionsnivån för direktivet om kritiska entiteters motståndskraft motsvarar kommissionens förslag och att direktivet är konsekvent med den politiska kompromissen om NIS2. Sammantaget kommer dessa åtgärder att öka motståndskraften och beredskapen genom ett mer samstämmigt och robust system med utförliga nationella planer för incident- och krishantering. Dessa åtgärder ingick även i kommissionens rekommendation om att bygga en **gemensam cyberenhet**|[14] från förra året. I rekommendationen anges hur de olika aktörerna i cybersäkerhetsekosystemet (diplomatkåren, poliskåren, civila aktörer och i förekommande fall försvaret) ska samarbeta på operativ nivå. Den nuvarande hotbilden visar värdet av ändamålsenligt samarbete mellan viktiga aktörer.

Kommissionen fortsätter att övervaka genomförandet av **verktygslådan för cybersäkerhet i 5G-nät**[15]. I detta sammanhang antog samarbetsgruppen för nät- och informationssäkerhet den 11 maj en rapport om säkerheten i Open RAN[16]. Samarbetsgruppen fortsätter även att arbeta med medlemsstaterna för att göra Europeiska kompetenscentrumet för cybersäkerhet fullt operativt.

Den 22 mars 2022 föreslog kommissionen nya regler för **gemensamma cybersäkerhets- och informationssäkerhetsåtgärder vid EU:s institutioner, organ och byråer**. Dessa regler kommer att stärka EU-förvaltningens motståndskraft och förmåga att reagera på cyberhot och cyberincidenter. Genom att samla dessa verksamheter i en gemensam ram stärks det interinstitutionella samarbetet och riskexponeringen minskar. Genom förslaget till **förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer**[17] kommer CERT-EU:s mandat att stärkas och en ny interinstitutionell cybersäkerhetsstyrelse att inrättas, samtidigt som cybersäkerhetskapaciteten stärks och regelbundna mognadsbedömningar av cybersäkerheten och bättre cyberhygien främjas. Den föreslagna **förordningen om informationssäkerhet i unionens institutioner, organ och byråer**[18] kommer att skapa en minimiuppsättning regler och standarder för säker hantering och säkert informationsutbyte för alla EU:s institutioner, organ och byråer. Detta ska säkerställa ett förstärkt och konsekvent skydd mot framväxande hot vad gäller information. Kommissionen uppmanar nu Europaparlamentet och rådet att snabbt anta dessa åtgärder.

Kommissionen har slutfört sitt offentliga samråd om åtgärder för att stärka digitala produkters **cyberresiliens** och arbetar nu med ett förslag som kommer att offentliggöras i höst[19]. Förslaget syftar till att hantera sårbarheten hos digitala produkter och tillhörande tjänster.

---

13 COM(2020) 829.

14 Rekommendation om att bygga en gemensam cyberenhet| /Att forma EU:s digitala framtid (europa.eu).

15 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

16 Samarbetsgruppen för nät- och informationssäkerhet, *Report on the cybersecurity of Open RAN*, 11.5.2022.

17 COM(2022) 122.

18 COM(2022) 119.

19 *EU-rättsakt om cyberresiliens – nya it-säkerhetsregler för digitala produkter och tillhörande tjänster* (europa.eu).

Digitala produkter och tillhörande tjänster skapar möjligheter för ekonomin och samhället i EU, men också nya utmaningar. När allt är uppkopplat kan en cyberincident påverka ett helt system och störa ekonomiska och sociala verksamheter.

Den 9 mars 2022 antog EU:s telekommunikationsministrar enhälligt Nevers-förklaringen om stärkande av EU:s cybersäkerhetskapacitet, där kommissionen uppmanas att ”inrätta en ny fond för nödåtgärder i samband med cyberhot”[20]. Kommissionen överväger hur befintliga fonder kan användas på bästa sätt för att stödja förebyggande åtgärder och krishantering.

Kritiska sektorer

En tryggad **energiförsörjning** för EU är avgörande för invånarnas välbefinnande och för att våra ekonomier ska fungera smidigt. Den nuvarande situationen visar på behovet av tydliga cybersäkerhetsregler inom denna sektor Kommissionen arbetar med en nätföreskrift för cybersäkerhet i gränsöverskridande elflöden enligt förordningen om m den inre marknaden för el[21], i syfte att tillhandahålla regler för riskbedömningar, gemensamma minimikrav, planering, övervakning, rapportering och krishantering. De avsedda målen för nätföreskriften om cybersäkerhet har blivit ännu mer relevanta sedan Rysslands anfallskrig mot Ukraina. Kommissionen har även inlett ett strukturerat samarbete mellan Enisa, Entso för el[22], Entso för gas[23] och energigemenskapen inom ramen för den regelbundna övervakningen av cybersäkerhetssituationen inom energisektorn.

EU har arbetat för att skydda partnerländernas säkerhet utan att skapa nya risker för EU i sig. Den akuta synkroniseringen mellan Ukrainas och Moldaviens elnät och det europeiska kontinentala nätet genomfördes i mars 2022, efter antagandet av riskreducerande åtgärder, särskilt vad gäller cybersäkerhet.

Kriget och sanktionerna har även skapat många problem för EU:s **transportsektor**, från säkerhetsrisker för EU:s civila luftfart och lastbilsförare som sitter fast i konfliktzoner, till förstörandet av Ukrainas transportinfrastruktur. Dess faktorer orsakar avbrott i leveranskedjorna och hotar den globala livsmedelstryggheten. Europeiska unionens byrå för luftfartssäkerhet (Easa) har i nära samarbete med kommissionen och Europeiska organisationen för säkrare flygtrafiktjänst (Eurocontrol) ända sedan kriget inleddes rekommenderat aktörer att inte flyga inom Ukrainas luftrum och undvika att använda luftrummet inom 100 sjömil från gränsen mellan Belarus/Ryssland/Ukraina.

Kommissionen har även arbetat för att stärka EU-transportsektorns beredskap och resiliens. Den nya beredskapsplanen för transportsektorn[24], som antogs den 23 maj, utgår från erfarenheterna både från covid-19-pandemin och Rysslands militära angrepp mot Ukraina. I beredskapsplanen för transportsektorn föreslås en verktygslåda med tio åtgärder som vägledning för medlemsstaterna när de inför svarsåtgärder vid nödlägen och kriser.

---

[20] ”08/03/2022 – Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique” – pressmeddelande – Frankrikes finansministerium (economie.gouv.fr).

[21] Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el (EUT L 158, 14.6.2019, s 54). Ett förslag granskas för närvarande av Byrån för samarbete mellan energitillsynsmyndigheter.

[22] Europeiska nätverket av systemansvariga för överföringssystemen för el (Entso för el).

[23] Europeiska nätverket av systemansvariga för överföringssystemen för gas (Entso för gas).

[24] COM(2022) 211.

Åtgärderna syftar bland annat till att säkerställa en miniminivå på förbindelserna, bygga upp motståndskraft mot cyber- och hybridhot och stärka samarbetet med internationella partner om krisberedskap och svarsåtgärder. I beredskapsplanen framhåller kommissionen även hur viktigt det är att man, tillsammans med relevanta byråer och organ eller andra aktörer, och med utgångspunkt i befintliga processer, genomför beredskapstest enligt olika krisscenarier.

Inom **EU-ramen för hälsosäkerhet** måste informationsutbytet via systemet för tidig varning och reaktion, inbegripet stöd till medicinska evakueringar från Ukraina, skyddas mot cyberattacker. Arbete pågår med att förbättra systemsäkerheten.

Samarbete med partner

EU fortsätter att samarbeta med sina internationella partner för att förebygga, avskräcka, motverka och bemöta skadligt beteende i cyberrymden. Samarbetet på detta område är viktigare än någonsin till följd av Rysslands anfallskrig mot Ukraina. I detta sammanhang har utrikestjänsten samarbetat med partner som Förenta staterna och Nato för att utbyta information om lägesuppfattning och samordna åtgärder för att motverka skadliga cyberverksamheter som riktas mot Ukraina och stödja Ukraina och andra länder i regionen för att säkerställa komplementaritet och undvika överlappningar.

EU:s redan dessutom intensifierat sitt redan nära samarbete med Förenta staterna inom ramen för handels- och teknikrådet mellan EU och USA. I det gemensamma uttalandet[25] efter ministermötet i Paris i maj betonade parterna handels-och teknikrådets centrala roll för det förnyade transatlantiska partnerskapet, som möjliggör samordning av gemensamma åtgärder från EU och Förenta staterna med anledning av Rysslands angrepp mot Ukraina. Båda parterna var överens om att nära samarbete för att öka leveranskedjornas resiliens är viktigare än någonsin. Dessutom inrättades en särskild arbetsgrupp för offentlig finansiering av säker och resilient digital infrastruktur i tredjeländer för att bana vägen för gemensam offentlig finansiering från Förenta staterna och EU av digitala projekt i tredjeländer, baserat på ett antal gemensamma övergripande principer.

Den strategiska kompassen som antogs i mars 2022 (se avsnitt VII) kommer ytterligare att stärka EU:s verktygslåda för cyberdiplomati och utveckla EU:s politik för it-försvar så att EU har en bättre beredskap för och kan bemöta cyberattacker på ett bättre sätt, som ett led i en bredare strategi för att stärka EU:s förmåga att agera i händelse av kriser och försvara sina intressen.

Cybersäkerhetsstöd till Ukraina och dess grannländer

EU arbetade redan före kriget med att stödja Ukrainas cyberresiliens. EU och Ukraina genomförde en första cyberdialog redan i juni 2021, och EU gav stöd till cybersäkerhet och en resilient digital omställning via programmet *EU4Digital Ukraine*, som har en budget på 25 miljoner euro. Ett ytterligare partnersamverkansprogram på 1,5 miljoner euro är avsett att hjälpa Ukrainas cybersäkerhetsinstitutioner att anpassa sig till EU:s standarder.

Efter krigsutbrottet främjar EU samarbete mellan cyberexperter från EU och Ukraina och samordnar tillhandahållande av tekniskt stöd, utrustning, programvara och tillhörande tjänster för att stärka Ukrainas cyberresiliens och cyberförsvar.

[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108.

EU bedömer även möjligt stöd på medellång sikt till Moldavien, Georgien och västra Balkan. Den 3-4 mars 2022 genomfördes ett gemensamt utvärderingsuppdrag till Moldavien om cybersäkerhetsbehov, vilket har lett till införandet av en särskild krishanteringsåtgärd för att snabbt öka cybersäkerheten i landet. Liknande krishanteringsåtgärder utformas för ett utvalt antal länder i västra Balkan, som anses vara särskilt utsatta för risker eftersom de har anslutit sig till EU:s sanktioner. Bedömningar görs även av eventuellt ytterligare stöd till Moldavien via den europeiska fredsfaciliteten.

III. ORGANISERAD BROTTSLIGHET OCH TERRORISM

Rysslands anfallskrig mot Ukraina har tvingat miljontals människor att lämna sina hem, vilket betydligt har ökat rörelserna över EU:s yttre gränser. Den 18 maj hade nästan sex miljoner människor kommit till EU från Ukraina och Moldavien, och hittills har 2,8 miljoner personer registrerats för tillfälligt skydd i EU. EU har arbetat för att mottagandet av de människor som flyr från kriget ska ske så snabbt och flexibelt som möjligt, utan att äventyra säkerheten vid EU:s yttre gränser. EU har vidtagit helt nya åtgärder för att erbjuda tillfälligt skydd till dem som flyr från kriget och hanterar alla nyanlända utan diskriminering. Samtidigt går det inte att bortse från de potentiella risker som kan uppstå när så många människor är i rörelse samtidigt. Med starkt stöd från berörda EU-organ övervakar EU därför ny utveckling i organiserad brottslighet och terrorism.

Ett starkt Schengenområde i en förvärrad hotbild

I och med den skärpta hotbilden till följd av kriget som pågår precis utanför EU:s yttre gräns är det viktigare än någonsin att säkerställa en hög säkerhetsnivå inom **Schengenområdet** och i EU.

I maj antog kommissionen den första rapporten om Schengenläget[26] för att genomföra den ambitiösa agendan för Schengenområdet som anges i strategin från juni 2021. Den årliga Schengencykeln utgör en ny styrningsmodell för Schengenområdet, med regelbundna hälsokontroller av Schengenläget. Hälsokontrollerna kommer att möjliggöra snabb identifiering av brister och effektiva uppföljningsförfaranden, med målet att förstärka Schengenområdet och göra det mer resilient.

I denna första rapport bekräftar kommissionen behovet av att stärka insatserna för att genomföra viktiga initiativ på EU-nivå, bland annat systematiska kontroller av alla resenärer vid de yttre gränserna och till fullo utnyttja Frontex och Europols mandat. I rapporten behandlas även förslag till och befintliga verktyg för gränsöverskridande polissamarbete.

Den nya arkitekturen för EU:s informationssystem för gränsförvaltning, migrationshantering och säkerhet och deras interoperabilitet är hörnstenen i insatserna för att förbättra den inre säkerheten och gränsförvaltningen. Ett ändamålsenligt genomförande av alla faktorer i interoperabilitetsramen enligt de överenskomna tidsfristerna kommer att vara avgörande i detta sammanhang.

[26] COM(2022) 301.

Vaksamhet och samordning

Starkare samarbete i fråga om brottsbekämpning mellan medlemsstaterna och med tredjeländer och åtgärder mot kriminella nätverk och kriminella personer som kan försöka utnyttja kriget mot Ukraina är avgörande för att säkerställa medvetenhet om framväxande brotts- och terroristhot. Medlemsstaterna och EU:s operativa partner delar aktivt relevant tillgänglig information och kriminalunderrättelser med Europol, som dubbelkontrollerar och analyserar informationen och omvandlar den till operativa anmälningar av underrättelser för åtgärder, t.ex. tidiga varningar och hotbildsbedömningar.

Organiserad brottslighet

Den organiserade brottsligheten finner redan vägar för att utnyttja den rådande situationen. I inledande underrättelseanalyser identifierades brottsmönster inom ett antal områden, bland annat människohandel, falska deklarationer för importerade och exporterade varor, nätbedrägeri, it-brottslighet och handel med skjutvapen. Det finns även bevis för att cyberbrottslingar som utger sig för att samla in pengar för Ukraina stjäl pengar och kryptovalutor[27]. Kriminella organisationer från Ukraina kan försöka omlokalisera sin brottsliga verksamhet till EU till följd av den nuvarande situationen.

Kommissionen, det franska EU-ordförandeskapet och EU:s RIF-byråer, särskilt Europol, har samarbetat för att mobilisera Europeiska sektorsövergripande plattformen mot brottshot (**Empact**) i syfte att bedöma, förutse, förebygga och motverka befintliga eller framväxande grova och organiserade brottshot. Den 7 april 2022 anordnade Europol ett Empact-möte som samlade företrädare och experter från EU-medlemsstaterna och EU:s säkerhetssektor. Mötet fokuserade på grova och organiserade brottshot som har uppstått till följd av kriget i Ukraina. De konkreta åtgärder som diskuterades omfattade bland annat insamling av mer underrättelseuppgifter, genomförande av operativa krishanteringsåtgärder och förnyad inriktning för befintliga åtgärder samt gemensamma aktionsdagar.

Celbet (tullexpertgruppen för östra och sydöstra landsgränsen) – ett samordningsprojekt som finansieras av kommissionen, följer utvecklingen vid gränsen som en del av sitt uppdrag att tillhandahålla operativt stöd och vägledning till tulltjänstemän. Celbet övervakar även tullbeslag vid gränsövergångarna vid EU:s gräns (Polen, Slovakien, Ungern och Rumänien) med Ukraina.

Brottslighet och terrorism

Även om inga omedelbara terroristhot än så länge har uppstått i EU i samband med Rysslands invasion av Ukraina står det klart att det krävs ökad vaksamhet.

[27] Googles hotanalysgrupp observerade att ett ökat antal hotaktörer utnyttjar kriget i Ukraina som ett lockbete i nätfiske- och sabotagekampanjer. Forskare vid internetsäkerhetföretaget Cyren rapporterar om ökade bedrägerier med kryptovalutor där man utnyttjar konflikten genom användning av falska donationswebbplatser.

De ökade riskerna för brottslighet och terrorism innebär att det är viktigt att medlemsstaterna använder relevanta EU-databaser som Schengens informationssystem för att registrera uppgifter där om så är nödvändigt och ta fram uppgifter under kontroller av personer som reser in i EU. Detta kommer att bidra till att säkerställa att personer som utgör ett hot mot EU:s inre säkerhet identifieras vid de yttre gränserna. EU-Lisa, Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, fortsätter att arbeta för att säkerställa att EU:s gränsförvaltningssystem är fullständigt tillgängliga och effektiva. I vägledning[28] till medlemsstaterna klargörs hur de ska balansera behovet av att säkerställa en smidig hantering av personer som anländer till den yttre gränsen samtidigt som de utför nödvändiga säkerhetskontroller.

Beredskap

Utöver vägledning och samordning har EU stärkt sin beredskap genom utstationeringar av EU-organens personal.

Europol har utstationerat operativa enheter i de EU-medlemsstater som gränsar till Ukraina. Enheterna består av Europols gästande tjänstemän från medlemsstaterna och Europol-experter i Ungern, Litauen, Polen, Rumänien och Slovakien samt Moldavien[29]. De gästande tjänstemännen från Europol stöder de nationella myndigheterna med fördjupade säkerhetskontroller vid EU:s yttre gränser. Europols experter ger stöd genom att samla in och bedöma information för att upptäcka brotts- och terroristhot, stödja utredningar och identifiera personer som utgör en risk genom att försöka ta sig in i EU. Dessa operativa enheter samlar in information som används i brottshotbedömningar som finns tillgängliga för medlemsstaterna. Insamlingen av underrättelseuppgifter hjälper Europol att förutse utveckling och samordna operativa åtgärder med EU-medlemsstaterna för att bemöta kriminella gruppers verksamheter som försöker utnyttja kriget i Ukraina. På så sätt kan Europol även utöka sitt aktiva engagemang med Ukrainas brottsbekämpande myndigheter via den ukrainska sambandsman som är utplacerad till Europols huvudkontor i Nederländerna.

Europeiska gräns- och kustbevakningsbyrån (**Frontex**) är också närvarande i medlemsstaterna och i EU:s grannländer för att stödja gränskontroller: fler än 2 100 gränsvakter är för närvarande utstationerade inom EU, i västra Balkan och i Moldavien. **Europeiska stödkontoret för asylfrågor** (**Easo**) har utstationerat nästan 750 anställda i EU:s sydliga medlemsstater och i Litauen för att stödja operativa verksamheter, förstärka mottagningskapaciteten och hjälpa till med asylförfaranden.

I linje med det gällande **Prümbeslutet**[30], som ger medlemsstaterna möjlighet att utstationera brottsbekämpande tjänstemän för gemensamma operationer såsom gemensamma patruller, skickade kommissionen och det franska EU-ordförandeskapet en gemensam skrivelse till alla medlemsstater för att identifiera behov och begära utstationering av poliser i syfte att bilda gemensamma patruller i de medlemsstater i främsta linjen och påverkas mest av den stora

[28] Kommissionens meddelande om operativa riktlinjer för förvaltning av de yttre gränserna i syfte att underlätta gränspassage vid gränserna mellan EU och Ukraina, 2022/C 104 I/01.

[29] Situationen per den 3 maj är att Europol har utstationerat en Europoltjänsteman och tre gästande tjänstemän i Slovakien, en Europoltjänsteman i Polen, en Europoltjänsteman och fyra gästande tjänstemän i Rumänien och två gästande tjänstemän i Ungern. En Europoltjänsteman och två gästande tjänstemän är utstationerade i Moldavien.

[30] 2008/615/RIF och 2008/616/RIF.

tillströmningen av människor som passerar gränsen till följd av kriget. Kommissionen kommer att finansiera dessa utstationeringar via fonden för inre säkerhet – polis.

Kampen mot människohandeln

EU har varit på alerten ända sedan de första dagarna av kriget när det gäller riskerna inom ett särskilt område av den brottsliga verksamhet som kan utnyttja de enorma förflyttningarna av människor som söker säkerhet i EU. Det har varit viktigt att förhindra människohandlare att rikta in sig på utsatta människor på flykt, som främst är **kvinnor och barn**, t.ex. genom falska erbjudanden om transport eller husrum.

I mars utfärdade Europol och Eurojust tidiga varningar till berörda nationella myndigheter om potentiell människohandel och utnyttjande av offer som anländer från Ukraina. Eurojust bidrar till att stärka informationsutbytet och påskynda det rättsliga samarbetet, även med Ukraina, och utredningar rörande människohandel har hänskjutits till byrån för samordning.

EU-samordnaren för kampen mot människohandel har haft möten med EU-nätverket av nationella rapportörer och motsvarande mekanismer, EU-organen för rättsliga och inrikes frågor och EU:s plattform för det civila samhället mot människohandel för att diskutera de åtgärder som krävs för att förhindra och bekämpa övergrepp och skydda offer. Utredningar om eventuella fall av människosmuggling har inletts i flera medlemsstater.

EU har agerat snabbt och energiskt för att säkerställa en samordnad reaktion på detta verkliga hot mot människor som behöver EU:s hjälp. Operativa riktlinjer[31], bland annat om problemet med människohandel, gavs snabbt till medlemsstater som tillämpar direktivet om tillfälligt skydd för att stödja människor som flyr från Ukraina. Som ett led i 10-punktsplanen för starkare europeisk samordning när det gäller att ta emot människor som flyr kriget i Ukraina[32], som lades fram vid rådets möte (rättsliga och inrikes frågor) den 28 mars 2022, har EU-samordnaren för kampen mot människohandel i samarbete med EU-organen och medlemsstaterna tagit fram gemensam plan för bekämpning av människohandel[33] för att förebygga människohandel. Planen inriktas särskilt på registrering av enheter och privatpersoner (inklusive volontärer) som vill hjälpa till genom att erbjuda husrum, transport och andra typer av hjälp och på bakgrundskontroller. Kommissionen har även samarbetat med Easo för att stödja arbetet med att upptäcka offer för människohandel när hälsoundersökningar erbjuds vid mottagningscentrum. Ensamkommande barn och barn som skilts från sina föräldrar riskerar särskilt att utsättas för övergrepp, sexuellt utnyttjande eller påtvingad brottslighet. De ovannämnda operativa riktlinjerna innehåller även vägledning för att hjälpa medlemsstaterna att hantera anländande, mottagande och stöd till barn, särskilt ensamkommande barn. För att öka medvetenheten bland dem som befinner sig i riskzonen har kommissionen även inrättat en särskild webbplats med ett avsnitt med praktiska råd om hur man undviker människohandlare.

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - SV - EUR-Lex (europa.eu).

[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en.

[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en.

Vissa åtgärder för att skärpa beredskapen har vidtagits speciellt som svar på de nya förhållandena med anledning av kriget, medan andra viktiga åtgärder härrör från lagstiftningsinitiativ som redan var planerade före Rysslands anfallskrig mot Ukraina.

Kommissionen välkomnar överenskommelsen i februari 2022 om **Europols** reviderade mandat[34]. När mandatet genomförs kan Europol bättre stödja medlemsstaterna i kampen mot organiserad brottslighet och terrorism. Europol kommer då att ha de rätta verktygen och garantierna för att stödja polisens analyser av stordata för att utreda brott och utforma banbrytande metoder för att hantera it-brott. Dessa ändringar kompletteras av en förstärkt dataskyddsram och starkare parlamentarisk kontroll och ansvarsskyldighet.

Den 8 december 2021 lade kommissionen fram ett paket om **polissamarbete**[35] som för närvarande är föremål för förhandlingar. Paketet kommer att stärka samarbetet mellan poliser i medlemsstaterna genom ett snabbare, enklare och säkrare informationsutbyte och ett stärkt och mer effektivt operativt polissamarbete ute på fältet. Kommissionen uppmanar Europaparlamentet och rådet att snabbt anta detta paket.

När dessa lagstiftningsförslag har antagits och genomförts kommer de att bidra till att stödja polisen i kampen mot gränsöverskridande organiserad brottslighet. Detta kommer att vara särskilt viktigt i ett sammanhang där kriminella organisationer från Ukraina kan försöka omlokalisera sin brottsliga verksamhet till EU till följd av den nuvarande situationen.

EU:s rådgivande uppdrag i Ukraina har sedan 2014 stöttat reformer av landets rättsvårdande institutioner. Uppdragets mandat sågs över i mars 2022 för att möjliggöra stöd vid Ukrainas gränsövergångar med Polen, Rumänien och Slovakien. Detta kommer att förbättra lägesuppfattningen om gränsöverskridande brottslighet, även när det gäller människohandel och flödet av humanitär hjälp till Ukraina.

IV. VAPEN, FARLIGA MATERIAL OCH KRITISKA INCIDENTER

Kriget har lett till att ett mycket stort antal skjutvapen och andra vapen är i omlopp i Ukraina, vilket utgör nya risker för EU och de andra länder som gränsar till Ukraina.

Vaksamhet och samordning

De operativa riktlinjer som utfärdades i mars innehåller råd till medlemsstaterna om hur de kan hantera utmaningen med den ökade spridningen av skjutvapen i ett läge med massiv tillströmning av människor vid EU:s gränser[36]. I riktlinjerna betonas att det är viktigt att kontinuerligt kontrollera förekomsten av skjutvapen och att ingen får resa in med vapen i EU utan vapentillstånd. När Ukrainas myndigheter rapporterar skjutvapen som saknade bör medlemsstaterna rapportera detta i Schengens informationssystem.

---

[34] COM/2020/796.

[35] COM/2021/780, COM/2021/782 och COM/2021/784.

[36] Meddelande från kommissionen om operativa riktlinjer för förvaltning av de yttre gränserna i syfte att underlätta gränspassage vid gränserna mellan EU och Ukraina, 2022/C 104 I/01.

Det är mycket viktigt att alla transporter av skjutvapen till Ukraina registreras korrekt, med alla relevanta uppgifter (typ, land och tillverkningsår, märke, modell, kaliber och serienummer) för att göra det lättare att spåra vapnen, både i Ukraina och EU.

EU har offentligen djupt beklagat Rysslands hänsynslösa angrepp mot och i omedelbar närhet av civila kärnkraftverk och biologi- och kemianläggningar i Ukraina och alla handlingar som äventyrar dessa anläggningars säkerhet. Kommissionen övervakar situationen i Ukraina med särskild uppmärksamhet på det radiologiska hotet, som är en mycket viktig fråga när det gäller EU:s inre säkerhet[37]. Kommissionen övervakar även potentiella kemiska hot och har inrättat en intern samordningsmekanism om snabba riskbedömningar behövs.

Beredskap

Enligt EU:s handlingsplan mot olaglig handel med skjutvapen 2020–2025 är Ukraina redan ett av de länder som anses vara prioriterade för särskilda insatser på extern nivå i EU. Inom ramen för Empact finns det även en särskild operativ insats för regionen, inbegripet Ukraina. Mot bakgrund av risken för att skjutvapen omdirigeras kommer det dock att krävas särskilda EU-finansierade projekt och operativt samarbete med Europol, Frontex och delen om skjutvapen i Empact. Kommissionen kommer inom kort att lägga fram ett förslag om översyn av förordningen om skjutvapen[38] när det gäller export, import och transitering av civila skjutvapen. Översynen ingår i den övergripande rättsliga och operativa ramen för att förebygga, upptäcka, utreda och lagföra olaglig handel med vapen.

För att förbättra EU:s beredskap för och insatser vid folkhälsorisker, såsom CBRN-hot, bygger kommissionen upp strategiska reserver av insatskapacitet via EU:s civilskyddsmekanism som finansieras av myndigheten för beredskap och insatser vid hälsokriser (Hera)[39]. Kommissionens avdelningar arbetar tillsammans för att ta fram ett strategiskt rescEU-beredskapslager på 540,5 miljoner euro. Lagret kommer att innehålla dels utrustning och läkemedel, vacciner och annan sjukvårdsmateriel för behandling av patienter som utsatts för CBRN-agenser, dels en dekontamineringsreserv inom rescEU-mekanismen för att tillhandahålla dekontamineringsutrustning och specialiserade insatsgrupper. Som ett omedelbart första steg har EU mobiliserat sitt rescEU-beredskapslager för läkemedel för att handla upp kaliumjodidtabletter, som kan användas för att skydda människor mot de skadliga effekterna av strålning, och andra sådana förnödenheter som Ukraina är i akut behov av. Nästan 3 miljoner jodidtabletter har redan levererats till Ukraina via EU:s civilskyddsmekanism, med hjälp från Frankrike och Spanien.

V. SAMORDNADE INSATSER FÖR ATT STÄLLA RYSSLAND TILL SVARS FÖR ANGREPPET

[37] Kommissionen kommer i samarbete med sina amerikanska partner att anordna en workshop om riskerna i samband med radiologiska material på sjukhus som inte omfattas av tillsyn.

[38] Europaparlamentets och rådets förordning (EU) nr 258/2012 av den 14 mars 2012 om genomförande av artikel 10 i FN:s protokoll om olaglig tillverkning av och handel med eldvapen, delar till eldvapen och ammunition, bifogat till Förenta nationernas konvention mot gränsöverskridande organiserad brottslighet (FN:s protokoll om skjutvapen), och om införande av exporttillstånd, import- och transiteringsåtgärder för skjutvapen, delar till skjutvapen och ammunition.

[39] Heras arbetsplan för 2022 (europa.eu).

EU spelar en avgörande roll i världssamfundets insatser för att utöva påtryckningar på Ryssland för att förmå landet att upphöra med sitt angrepp mot den ukrainska staten och de civila som har blivit inblandade i konflikten. Detta är oacceptabelt och strider mot internationell rätt. Påtryckningarna omfattar åtgärder för att informera förövarna om konsekvenserna av deras handlingar, bland annat stränga sanktioner och åtgärder för att identifiera och underlätta lagföring av krigsförbrytelser.

Restriktiva åtgärder och förverkande av tillgångar

Sedan Rysslands erkännande av de icke-regeringskontrollerade områdena i länen Donetsk och Luhansk i Ukraina den 21 februari 2022 och invasionen av Ukraina den 24 februari 2022 har EU infört de mest omfattande restriktiva åtgärderna någonsin gentemot Ryssland. Hittills har fem sanktionspaket antagits. Åtgärderna fokuserar på viktiga sektorer, inklusive finans-, handels-, transport-, försvars- och mediesektorn, och riktar sig mot den politiska och militära eliten samt framträdande ryska och belarusiska oligarker. Förteckningarna omfattar redan fler än 1 000 personer och 80 enheter. Ett sjätte sanktionspaket diskuteras för närvarande i rådet.

Effekterna av dessa och tidigare restriktiva åtgärder gentemot personer och företag i Ryssland och Belarus kommer att bli lika starka som genomförandet. Samordning på EU-nivå kan bidra stort till att täppa till eventuella luckor och kommissionen har gett omfattande stöd till berörda aktörer via skriftlig vägledning. möten med aktörerna, en särskild expertgrupp och en rad olika resurser för att underlätta efterlevnaden.

Kommissionen har även tillsatt en arbetsgrupp för frysning av tillgångar (*Freeze and Seize Task Force*) som sammanför kommissionens avdelningar, medlemsstaterna, Eurojust och Europol. Hittills har medlemsstaterna rapporterat att de har fryst tillgångar värda 9,89 miljarder euro[40]. Den 11 april inledde Europol insatsen Oscar tillsammans med medlemsstaterna, Eurojust och Frontex för att stödja finansiella utredningar och brottsutredningar avseende kriminella tillgångar som ägs av personer och juridiska enheter som omfattas av EU:s sanktioner i samband med Rysslands krig mot Ukraina. EU:s arbetsgrupp för frysning av tillgångar samarbetar nära med arbetsgruppen REPO (*Russian Elites, Proxies, and Oligarchs*) som har inrättats av G7-länderna (Frankrike, Förenade kungariket, Förenta staterna, Italien, Japan, Kanada och Tyskland) och likasinnade partner som Australien samt arbetsgruppen *US KleptoCapture* och den ukrainska arbetsgruppen.

Arbetsgruppen för frysning av tillgångar fungerar som en plattform för att samordna och underlätta utbytet av information och erfarenheter mellan medlemsstaterna, ge vägledning om genomförandet av sanktioner och underlätta utbytet av bästa praxis om brottsutredningar och förverkande av tillgångar. Det är särskilt viktigt att de brottsbekämpande myndigheterna är vaksamma och agerar proaktivt när det gäller eventuella brott som begås av de personer och enheter som omfattas av sanktionerna. Arbetsgruppen vill också föra en diskussion om ett eventuellt utnyttjande av förverkade tillgångar, t.ex. för att bidra till återuppbyggnaden av Ukraina.

Kommissionen antar i dag ett **paket om återvinning och förverkande av tillgångar**[41],som utgår från lärdomarna från genomförandet av unionens restriktiva åtgärder mot ryska och belarusiska personer och enheter. Paketet kommer att underlätta ett ändamålsenligt

[40] Det finns även blockerade tillgångar på omkring 23 miljarder euro som tillhör den ryska centralbanken.
[41] COM(2022) 245.

genomförande av EU:s restriktiva åtgärder genom att möjliggöra snabb spårning och identifiering av egendom som ägs eller kontrolleras personer eller enheter som omfattas av sådana åtgärder. Den förstärkta ramen för återvinning och förverkande av tillgångar kommer även att tillämpas på överträdelser av de restriktiva åtgärderna, och kommer således att säkerställa ändamålsenlig spårning, frysning, hantering och förverkande av vinning som härrör från överträdelser av de restriktiva åtgärderna. För att säkerställa att tillgångar som ägs av personer och enheter som överträder de restriktiva åtgärderna verkligen kan förverkas antar kommissionen i dag även förslag till ett rådsbeslut om att lägga till överträdelser av sanktioner i förteckningen över EU-brott i artikel 83.1 i EUF-fördraget[42], åtföljt av ett meddelande[43]. Syftet är att föreslå ett direktiv för att åstadkomma en tillnärmning när det gäller fastställande av brottsrekvisit och påföljder för överträdelser av restriktiva åtgärder.

Mer generellt utgör detta paket ett viktigt steg i kampen mot organiserad brottslighet. Det är ett led i kommissionens åtagande i strategin för EU:s säkerhetsunion och strategin för att bekämpa organiserad brottslighet 2020–2025[44]. I paketet föreslår kommissionen en översyn av 2014 års direktiv om förverkande, rådets beslut från 2007 om kontor för återvinning av tillgångar och 2005 års rambeslut om förverkande av vinning, hjälpmedel och egendom som härrör från brott. Syftet är att stärka kapaciteten för spårning, identifiering och förverkande av olagliga intäkter för att lösa problemet med den mycket låga graden av förverkande i EU[45]. Genom paketet utökas antalet brott som omfattas och reglerna för förverkande utvidgas till att omfatta fall där det inte är möjligt att lagföra ett visst brott men det står klart att tillgångarna härrör från brottslig verksamhet. Översynen kommer även att bidra till att stärka en ändamålsenlig hantering av frysta och förverkade tillgångar och till kapaciteten för kontoren för återvinning av tillgångar att spåra och identifiera olagliga tillgångar. EU:s nya ram för återvinning av tillgångar är utformad för att hantera kriminella organisationers komplexa tillvägagångssätt. De verkar ofta över gränserna och använder olika metoder för att dölja sina tillgångar, bland annat i form av kryptotillgångar.

Samordnade rättsliga åtgärder

EU har även arbetat för att säkerställa samordnade rättsliga åtgärder mot **internationella brott** som ska ha begåtts i Ukraina, så att förövarna ställs till svars.

Två medlemsstater och Ukraina har tillsatt en gemensam utredningsgrupp för att utreda krigsbrott, brott mot mänskligheten och andra internationella brott som ska ha begåtts på ukrainskt territorium. Eurojust tillhandahåller rättsligt, analytiskt, ekonomiskt och logistiskt stöd till stöd för den gemensamma utredningsgruppen. Den 25 april 2022 anslöt sig åklagarkontoret vid Internationella brottmålsdomstolen till den gemensamma utredningsgruppen som deltagare[46] och ytterligare deltagare förväntas ansluta sig inom kort.

Den 25 april 2022 lade kommissionen fram ett förslag om ändring av Eurojustförordningen[47] för att Eurojust ska kunna bevara, analysera och lagra bevis för centrala internationella brott.

---

[42] COM(2022) 247.
[43] COM(2022) 249.
[44] COM(2021) 170.
[45] Enligt Europols uppskattningar har endast 2 % av kriminella tillgångar frysts (2,4 miljarder euro) och 1 % har förverkats (1,2 miljarder euro) trots att intäkterna från kriminell verksamhet på de största kriminella marknaderna i EU uppgick till 139 miljarder euro 2019 (1 % av EU:s BNP).
[46] https://www.eurojust.europa.eu/eurojust-and-the-_war-in-ukraine.
[47] COM(2022) 187 final.

Eurojust och Europol kommer att fortsätta sitt nära samarbete under denna process. Nätverket mot folkmord har även en avgörande roll i samordningen av de rättsliga åtgärderna. Eurojust svarar för nätverkets sekretariat, som har tagit fram en atlas över icke-statliga organisationer som för närvarande är verksamma i Ukraina. Sekretariatet stöder även aktörer från medlemsstaterna och Ukraina som utreder aktiva fall med anknytning till kriget.

I april 2022 reviderade rådet ytterligare mandatet för **EU:s rådgivande uppdrag i Ukraina**, vilket ger uppdraget möjlighet att stödja de ukrainska myndigheterna i utredningar och lagföring av eventuella internationella brott som begåtts i samband med Rysslands militära angrepp. Uppdraget kommer att ge de ukrainska myndigheterna strategisk rådgivning om utredning och lagföring av internationella brott, nödvändiga ändringar av den ukrainska lagstiftningen, kommunikationsstrategier och utbildning i relaterade frågor. Uppdraget ingår i ett antal samordningsinitiativ i detta sammanhang och ingår tillsammans med EU-delegationen i Förenta staternas och EU:s rådgivande grupp om massövergrepp i Ukraina.

VI. UTLÄNDSK INFORMATIONSMANIPULATION OCH INBLANDNING

Den nuvarande geopolitiska utvecklingen visar på riskerna för utländsk inblandning. Rysslands militära angrepp mot Ukraina har åtföljts av **informationsmanipulation och inblandning**. Grundlösa påståenden om ”nazism” och ”folkmord” mot Ukrainas regering, falska flaggoperationer och ogrundade anklagelser mot Nato och västvärlden har använts för att motivera de brutala attackerna mot Ukraina, samtidigt som yttrandefriheten och den oberoende rapporteringen i Ryssland har förtryckts. Det finns en kontinuerlig risk i form av manipulerat audiovisuellt material och desinformation som Ryssland kan försöka utnyttja som en förevändning för ytterligare militära attacker och för att försvaga det ukrainska motståndet, splittra världssamfundet i dess motstånd mot kriget eller så tvivel om Rysslands kränkningar av internationell rätt. I den strategiska kompassen förklarar EU att unionen kommer att reagera med kraft på utländsk informationsmanipulering och inblandning och förstärka sin motståndskraft för och förmåga att motverka sådana hot[48]. Manipulation av den demokratiska diskussionen inom EU behandlas i EU:s handlingsplan för demokrati, kommissionens samordnade plan för att hantera desinformation och stärka demokratins motståndskraft[49].

Vaksamhet och samordning

EU reagerade med beslutsamma och samordnade åtgärder mot Rysslands desinformationskampanj i samband med det militära angreppet på Ukraina. EU har samarbetat nära med medlemsstaterna via systemet för snabb varning och med internationella partner som Nato, Förenta staterna, Kanada och G7-gruppens mekanism för snabba insatser för att utbyta insikter i de manipulationstrender och den taktik som Kreml använder. Arbetet med att bryta ned Kremls manipulation har intensifierats, särskilt via webbplatsen EUvsDisinfo, som sänder på engelska, ryska, ukrainska och andra språk för att tillhandahålla faktauppgifter inom EU, i Ukraina och i regionen och i Ryssland. De ryska statsägda mediekanalerna RT:s och Sputniks tv-sändningar som görs i eller som är riktade mot EU avbröts den 2 mars i och med de restriktiva åtgärder som EU vidtagit. Onlineplattformar, ledande sociala nätverk, annonsörer och aktörer i reklambranschen som har skrivit under

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/sv/pdf.

[49] COM(2020) 790.

uppförandekoden om desinformation[50] vidtar snabba åtgärder för att begränsa desinformation i samband med Rysslands angrepp mot Ukraina. Kommissionen och utrikestjänsten övervakar dessa insatser. De uppgifter som har inkommit visar att plattformarna har stärkt sin övervakning och sina verktyg för ingripande vad gäller kriget.

Dessutom vidtas snabba åtgärder för att stödja länder i Centralasien och västra Balkan för att stärka informationsresiliensen och motverka utländsk informationsmanipulering och desinformation.

Beredskap

Öppen användning av utländsk informationsmanipulering och inblandning, där desinformation ingår som ett av hybridhoten, innebär att det är ännu mer brådskande att följa upp EU:s handlingsplan för demokrati. Under de senaste månaderna har EU-institutionerna stöttat medlemsstaterna när det gäller att motverka utländsk informationsmanipulering och inblandning, särskilt inom ramen för systemet för snabb varning, genom att utbyta insikter om den taktik som sådana aktörer använder och om åtgärdsstrategier. Diskussioner om att ytterligare stärka EU:s allmänna åtgärder mot utländsk informationsmanipulering och inblandning pågår utifrån ett diskussionsunderlag från utrikestjänsten om att ta fram en särskild **verktygslåda** för att hantera detta hot. I och med detta samlas alla befintliga interna åtgärder och nya EU-verktyg inom den gemensamma utrikes- och säkerhetspolitiken. Detta kommer även att stödjas av de intensifierade åtgärder som vidtas av utrikestjänstens avdelning för strategisk kommunikation (Stratcom)[51] och av kommissionen.

Det europeiska observatoriet för digitala medier har tillsatt en arbetsgrupp om desinformation till följd av krigsutbrottet i Ukraina och samordnar åtgärder med hjälp av faktagranskare och forskare i sitt nätverk. Arbetsgruppen har undersökt hur personer som spred covid-konspirationsteorier snabbt inriktade sig på att börja sprida proryska lögner, en förändring som observerats i ett antal medlemsstater[52].

Syftet med förslaget till rättsakt om digitala tjänster är att möjliggöra snabb anpassning till utvecklingen av digital teknik och de tekniska och demokratiska utmaningar som detta medför, t.ex. hatpropaganda, desinformation på nätet och destabiliseringsstrategier. Europaparlamentet och rådet har gjort viktiga framsteg i förhandlingarna, vilket bör möjliggöra ett snabbt antagande av paketet.

VII. BREDARE BEREDSKAP

Vid en tidpunkt då kriget återvänt till Europa och en tid av stora geopolitiska förändringar har EU lagt in en högre växel i sin säkerhetssamordning med hjälp av initiativ som redan var

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[51] Europeiska utrikestjänstens avdelning för strategisk kommunikation, arbetsgrupper och informationsanalys tillhandahåller strategiskt kommunikationsstöd för genomförandet av EU:s utrikes- och säkerhetspolitik i berörda prioriterade regioner (det södra och östra grannskapet, västra Balkan) genom att utforma och genomföra särskilda strategiska kommunikationsåtgärder som inriktas på att främja EU:s politik, värden, mål och intressen.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.

planerade före Rysslands anfallskrig mot Ukraina. Initiativ som främst inriktas på EU:s yttre säkerhet har en stor inverkan på säkerhetsunionens inre dagordning.

Den 15 februari 2022 lade kommissionen fram **försvarspaketet**[53] med ett antal initiativ på områden som är avgörande för EU:s försvar och inre säkerhet. Detta bidrag från kommissionen till EU:s försvar och säkerhet täcker alla befintliga utmaningar. Paketet innehåller förslag på konkreta åtgärder mot en mer integrerad och konkurrensutsatt europeisk försvarsmarknad, vilket i synnerhet ska uppnås med hjälp av stärkt samarbete inom EU och stordriftsfördelar. Paketet innehåller även en färdplan om kritiska tekniker för säkerhet och försvar för att främja forskning, teknisk utveckling och innovation inom dessa sektorer och minska beroendet av kritiska tekniker och värdekedjor. Det syftar även till att stärka militär användning av rymden på EU-nivå. I paketet undersöker kommissionen även hur den kan öka insatserna mot hybridhot, även på cyberområdet, stärka den militära rörligheten inom och utanför Europa och vilka ytterligare åtgärder som kan vidtas för att hantera klimatutmaningar på försvarsområdet. För att komplettera detta arbete behandlar det gemensamma meddelandet **om analysen av investeringsgapet på försvarsområdet och vidare åtgärder**[54] av den 18 maj kapacitets- och investeringsgapet, som måste åtgärdas för att stödja de mest utsatta medlemsstaterna och fastställa åtgärder för att åtgärda de identifierade bristerna.

EU:s motståndskraft mot dessa hot kräver även kapacitetsstyrda strategier inom säkerhetssektorerna, vilket förespråkas i kommissionens handlingsplan för synergieffekter mellan civil industri, försvarsindustri och rymdindustri[55]. Arbete pågår med att främja kapacitetsstyrda strategier på området inre säkerhet och brottsbekämpning.

Den 21 mars 2022 antog rådet en **strategisk kompass för säkerhet och försvar**[56], som kort därefter godkändes av Europeiska rådet. Kompassen innehåller en ambitiös åtgärdsplan för att stärka EU:s säkerhets- och försvarspolitik till 2030. Målet är att göra EU till en starkare säkerhetsgarant med större förmåga som skyddar sina medborgare och bidrar till internationell fred och säkerhet. Kompassen innehåller konkreta förslag med en mycket exakt tidtabell för genomförandet i syfte att förbättra EU:s förmåga att agera beslutsamt vid kriser.

Ett av resultaten av den strategiska kompassen är en **EU-verktygslåda för hantering av hybridho**t som bör utgöra en ram för en samordnad reaktion på hybridkampanjer som påverkar EU och dess medlemsstater och kommer att omfatta inre och yttre åtgärder. Sektorsspecifika utgångspunkter för resiliens identifierades i början av 2022[57] och kommer att följas av en analys av brister och behov. Det är inom denna ram som EU kommer att fortsätta att bygga upp beredskap, motståndskraft och åtgärder mot hot till följd av Rysslands angrepp och eventuella andra försök att destabilisera demokratier och den regelbaserade multilaterala världsordningen.

---

53 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en.

54 JOIN(2022) 24.

55 COM(2021) 70.

56 *En strategisk kompass för säkerhet och försvar – För ett EU som skyddar sina medborgare, värden och intressen och bidrar till internationell fred och säkerhet*: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/sv/pdf.

57 SWD(2022) 21 final.

VIII. FRAMTIDSUTSIKTER

I framtiden måste EU vara ytterst vaksam på framväxande hot och bygga upp sin **beredskap för och motståndskraft mot** alla tänkbara scenarier. Krigets återverkningar kan ta sig olika uttryck och det är ännu inte möjligt att bedöma alla konsekvenser.

Omfattningen av ukrainska kriminella nätverks förflyttningar är ännu inte känd. Eurojusts tidigare arbete visar på en trend för handel med heroin från Afghanistan till EU via Ukraina, vilket har bekräftats av Europeiska centrumet för kontroll av narkotika och narkotikamissbruk (ECNN)[58]. De instabila förhållandena kan försvåra åtgärder mot heroinhandeln via denna rutt, vilket skapar en risk för ett eventuellt ökat inflöde av narkotika till EU.

Vissa risker för EU kommer sannolikt att öka i slutet av eller under eventuella avbrott i striderna. Spridningen av skjutvapen kommer att ägnas särskild uppmärksamhet, eftersom risken ökar när striderna i Ukraina avtar. Tidigare erfarenheter visar även att det finns en risk för att återvändande utländska stridande som har fått stridserfarenhet och kan ha kommit i kontakt med extremistgrupper i ett senare skede kan utföra terroristaktioner i EU. Detta potentiella fenomen bör övervakas noggrant och kommissionen underlättar redan diskussioner mellan medlemsstaterna om utmaningarna i samband med återvändande utländska frivilliga med en våldsam extremistisk bakgrund.

Mot bakgrund av dessa möjliga hot är det viktigt att strategin för EU:s säkerhetsunion fortsätter att genomföras tillsammans med andra viktiga strategier såsom EU:s strategi för cybersäkerhet, strategin för att bekämpa organiserad brottslighet (2021–2025), EU-agendan för terrorismbekämpning (2020–2025), EU:s handlingsplan mot olaglig handel med skjutvapen (2020–2025), EU:s strategi för bekämpning av människohandel (2021–2025) och EU:s strategi mot narkotika (2021–2025).

Insatserna för att förse EU med den nödvändiga lagstiftningsramen kommer att fortsätta. Kommissionen arbetar till exempel med en konsekvensbedömning för ett förslag om reglering av saluföring och användning av högriskkemikalier.

IX. SLUTSATS

Säkerhetsunionen fyller även fortsättningsvis sin funktion att förbereda EU och dess medlemsstater för att hantera befintliga och potentiella hot. Rysslands anfallskrig mot Ukraina har visat hur snabbt teoretiska hot kan förverkligas och visar på betydelsen av vaksamhet, samordning och beredskap.

Den fjärde lägesrapporten om genomförandet av EU:s strategi för en säkerhetsunion visar att EU kan anpassa sig, även vid exceptionella och oväntade hot som Rysslands anfallskrig mot Ukraina. Ett beslutsamt genomförande av strategin för EU:s säkerhetsunion är viktigare än någonsin.

---

[58] *Report on the drug and alcoholic situation in Ukraine for 2020* (enligt uppgifter från 2019), OEDT, *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery*, 2021/00446, Eurojust, maj 2020.